SSN Lab Assignment:
TLS

Task 1 - TLS handshake

Inspect TLS handshake:

1. Using *openssl* , establish a TLS connection to *facebook.com* . Look at the parameters of your connection and briefly describe them in your report.
2. Establish the connection again and intercept TLS handshake using *tcpdump/ wireshark*. Describe all packets involved in the TLS connection in your report.
3. What version of TLS is used? Describe which versions are not safe to use and under which conditions.
4. What ciphersuite is used? Make a small list of ciphersuite that you would recommend to use and why.

Task 2 - Man In The Middle

1. Setup a TLS proxy - *mitmproxy*
    a. There are several modes it can operate. You should use transparent mode.
    b. Describe setup steps and show that are able to read transmitted data.
2. Intercept TLS handshake before proxy and after proxy and describe how MITM is performed.
    a. When do you think TLS proxy is used for security purposes in the industry?
    b. What are techniques that are used to protect applications (desktop, web, mobile, etc.) from TLS proxying?
3. Proxy allows you not only to read data, but also modify it on the fly. Think of a scenario when it can be dangerous and try to demonstrate that.

Task 3 - x509

By default, mitmproxy uses its own certificate authority to issue certificates and if you inspect the certificate chain (f.e in browser) you will see that it looks suspicious.
Here you will try to create a certificate chain that looks almost the same as the original certificate chain for a website and, alongside, get familiar with common attributes that are used in x509 certificates.

1. Obtain a cert chain for *www.facebook.com* (f.e. using openssl):
   a. Does the cert chain contain the root cert? Where are trusted certs stored?
   b. Extract certs and place: root CA in *root.crt*, intermediate CA in *int_ca.crt,* and server cert in *server.crt.*
2. Using the contents of obtained certificates, create your own chain that mimics the original one, they should look almost identical.
   a. Document your steps and describe the meaning of certificates attributes.
   b. Include created certificate chain into the report as appendix - both in base64 and human readable form.
3. BONUS: Provide a server key and certificate to mitmproxy and try to visit *www.facebook.com* using the browser and check how the certificate chain is looking now (do not forget to add the created root CA certificate to the trusted store).